IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

CONNIE HOWARD, YADIRA YAZMIN HERNANDEZ, and DEBORAH REYNOLDS, on behalf of themselves and all others similarly situated, Plaintiffs, v. LABORATORY CORPORATION OF AMERICA and LABORATORY CORPORATION OF AMERICA HOLDINGS, Defendants.	)	Case No. 1:23-CV-00758

ORDER AND RECOMMENDATION OF
UNITED STATES MAGISTRATE JUDGE

This case arises from Defendants Laboratory Corporation of America's and Laboratory Corporation of America Holdings' (hereinafter "Defendants") use of "Meta Pixel" and "Google Analytics" on the Labcorp website. Plaintiffs Connie Howard, Yadira Yazmin Hernandez, and Deborah Reynolds (hereinafter "Plaintiffs") bring this proposed class action against Defendants alleging violations of the California Information Privacy Act and the Pennsylvania Wiretapping and Electronic Surveillance Control Act. This matter is before the Court on Defendants' Motion to Dismiss Plaintiffs' Amended Complaint [Doc. #78]. Defendants seek to dismiss Plaintiffs' claims against them for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1) and failure to state a claim

upon which relief may be granted pursuant to Federal Rule of Civil Procedure 12(b)(6). For the reasons set forth below, the Court recommends that Defendants' Motion be denied.

I. FACTS, BACKGROUND, AND PROCEDURAL HISTORY

Plaintiffs Howard and Hernandez are residents of California who have had Meta/Facebook and Google online accounts during all times relevant to Defendants' conduct in this case. (Am. Compl. [Doc. #67] ¶¶ 7-8, 83, 85, 89, 91.) Plaintiff Reynolds is a resident of Pennsylvania who likewise has had Meta/Facebook and Google accounts during all relevant times. (Am. Compl. ¶¶ 9, 95, 97.) Defendants maintain a website that "permits individuals to access their medical testing results, book medical testing appointments, request medical testing supplies, and pay for Labcorp services they have received." (Am. Compl. ¶ 54.) The Labcorp website also allows users to use its "search bar to look for medical information, including information concerning specific medical tests." (Am. Compl. ¶ 55.) As alleged in the Complaint, all three Plaintiffs used the Labcorp website to conduct text searches for sensitive medical issues at some point between approximately May 2021 and February 2023. (Am. Compl. ¶¶ 83-84, 89-90, 95-96.) The Complaint alleges that during the time that Plaintiffs conducted these searches, Defendants had deployed the Meta Pixel, Google Analytics, and other third-party tracking tools on their website. (Am. Compl. ¶¶ 2, 27, 47-48, 56, 58, 75.)[1]

The Complaint alleges that, when deployed on a website, the Meta Pixel and Google Analytics tracking tools act as business tools that allow Meta and Google, respectively, to use customers' identity, data, metadata, and search history to better target ads to them and similar

[1] While the exact date that Defendants placed these tracking tools on their website is unclear from the Amended Complaint, Plaintiffs allege that, at a minimum, these tracking tools were deployed during the time period that Plaintiffs interacted with Defendants' website. (Am. Compl. ¶¶ 2, 54-56.)

individuals based on the information obtained about them. (Am. Compl. ¶¶ 2-3, 13, 22-25, 28-34, 38-39, 42-45, 49-53, 59-74.) "In all websites where the Pixel operates, when a user exchanges information with the host of that site—such as through a search query—Meta's software script surreptitiously directs the user's browser to send a separate message to Meta's servers" containing the content that was sent to the host site along with personal identifiers allowing Meta to link the information to a particular Facebook account and then use that information for advertising and other purposes, including sale to other third parties. (Am. Compl. ¶¶ 28, 29, 32-37.) "Like the Meta Pixel, when a user exchanges information with the host of a website—such as through a search query—Google Source Code operates to surreptitiously direct[] the user's browser to send a separate message to Google's servers" containing the content that was sent to the host site along with personal identifiers allowing Google to link the information to a specific Google account and then use that information for advertising and other purposes. (Am. Compl. ¶¶ 45, 49-53.)

As a result of Defendants' deploying these tracking tools on their website, each time Plaintiffs searched the Labcorp website for their "sensitive medical issues," Defendants permitted Meta and Google to receive the content of the searches as well. (Am. Compl. ¶¶ 83-84, 86-87, 89-90, 92-93, 95-96, 98-99.) A fair reading of these allegations at the Motion to Dismiss stage is that the transmission of search queries by the tracking tools is not selective but rather automatic and occurred during each search conducted by Plaintiffs while the tracking tools were deployed on the Labcorp website. These tracking tools would explicitly link and identify the users' Facebook ID or Google ID with their search terms, and examples

of these searches are ones performed for "cancer colorectal patient," "billing," "colon cancer," and "pregnancy." (Am. Compl. ¶¶ 60, 64, 66, 74.)

Plaintiffs allege that, in part because of how the tracking tools are embedded, they were not aware that the tracking tools were present on the Labcorp website and therefore did not consent to the collection or automatic forwarding of any of their information or search queries to Meta or Google. (Am. Compl. ¶¶ 3, 25, 41, 76-77, 88, 94, 100.)

Plaintiffs originally brought a Complaint against Defendants and Meta Platforms, Inc., in the Northern District of California. Plaintiffs then consented to Meta's motion to sever, and the claims against it were joined to a related consolidated action in that same District, In re Meta Pixel Healthcare Litigation, No. 3:22-cv-03580-WHO (N.D. Cal. June 17, 2022) [Doc. #33, #52]. Because Meta was no longer a Party to the action, Plaintiffs and Defendants filed a joint stipulation to transfer the matter to this District, where Defendants are based [Doc. #54]. When the matter was transferred to this District, Defendants had a pending motion to dismiss [Doc. #53]. After the transfer, Plaintiffs filed an Amended Complaint against Defendants [Doc. #67], thereby rendering Defendants' prior motion to dismiss moot.

Plaintiffs' Amended Complaint brings two claims based on the above-alleged conduct: (1) a violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630-638; and (2) a violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701, *et seq.* Defendants have now moved to dismiss Plaintiffs' Amended Class Action Complaint for lack of standing and failure to state a claim.

II. STANDARDS OF REVIEW

A. Rule 12(b)(1)

Federal courts are courts of limited jurisdiction. Exxon Mobil Corp. v. Allapattah Servs. Inc., 545 U.S. 546, 552 (2005). Under Federal Rule of Civil Procedure 12(b)(1), a party may seek dismissal based on the court's "lack of subject-matter jurisdiction." Subject matter jurisdiction is a threshold question that raises the issue of "whether [the plaintiff] has a right to be in the district court at all and whether the court has the power to hear and dispose of [the] claim." Holloway v. Pagan River Dockside Seafood, Inc., 669 F.3d 448, 452 (4th Cir. 2012); see also Constantine v. Rectors & Visitors of George Mason Univ., 411 F.3d 474, 479-80 (4th Cir. 2005).

A party invoking a federal court's jurisdiction must demonstrate standing. To overcome the standing threshold, and thereby survive a 12(b)(1) motion to dismiss, a plaintiff must demonstrate "a personal stake in the outcome of the controversy" that is sufficient to warrant the "invocation of federal court jurisdiction." Summers v. Earth Island Inst., 555 U.S. 488, 493 (2009). "To establish standing at the motion to dismiss stage a plaintiff must plausibly allege that: (1) it has suffered an injury in fact that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." Liberty Univ., Inc. v. Lew, 733 F.3d 72, 89 (4th Cir. 2013) (internal quotation omitted). Further, the plaintiff must establish standing for each claim and each form of relief she seeks. TransUnion LLC v. Ramirez, 594 U.S. 413, 431 (2021).

Parties bring what is called a facial challenge under Rule 12(b)(1) when they assert, as Defendants do here, that a complaint alleges facts that, even if taken as true, do not establish subject matter jurisdiction. See Kerns v. United States, 585 F.3d 187, 192 (4th Cir. 2009); Doe v. United States, 381 F. Supp. 3d 573, 590 (M.D.N.C. 2019). In reviewing a facial challenge under Rule 12(b)(1), a district court should afford plaintiffs the same procedural protection as they would receive under Rule 12(b)(6) consideration. Kerns, 585 F.3d at 192-93; see also Willner v. Dimon, 849 F.3d 93, 99 (4th Cir. 2017); Wikimedia Found. v. Nat'l Sec. Agency, 857 F.3d 193, 208 (4th Cir. 2017) ("A defendant may challenge standing at the motion-to-dismiss stage in one of two ways: facially or factually. In a facial challenge, the defendant contends that the complaint fails to allege facts upon which standing can be based, and the plaintiff is afforded the same procedural protection that exists on a motion to dismiss." (internal quotations, citations, and brackets omitted)). This means both that "the facts alleged in the complaint are taken as true, and the motion must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction," Kerns, 585 F.3d at 192-93, and that the district court should "construe all reasonable inferences in the manner most favorable to the plaintiff," Dodge v. VT Inc., No. Civ.1:02CV00706, 2003 WL 203167, at *2 (M.D.N.C. Jan. 27, 2003) (citing Robinson v. Overseas Mil. Sales Corp., 21 F.3d 502, 507 (2d Cir. 1994)); Kirkcaldy v. Richmond Cnty. Bd. of Educ., 212 F.R.D. 289, 294 (M.D.N.C. 2002) (same); accord Ctr. for Env't Health v. Regan, No. 7:22-CV-00073-M, 2023 WL 3192322, at *7 (E.D.N.C. Mar. 30, 2023) (court should draw all reasonable inference in the plaintiff's favor in a facial 12(b)(1) challenge).

B. Rule 12(b)(6)

Defendants also move to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), contending that Plaintiffs have failed to state a claim upon which relief can be granted. "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). This standard does not require "detailed factual allegations," but it demands more than "an unadorned, the-defendant-unlawfully-harmed-me accusation." Id. A claim is facially plausible when the plaintiff provides enough factual content to enable the court to reasonably infer that the defendant is liable for the misconduct alleged. Id. "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." Id. In this way, Rule 12(b)(6) protects against meritless litigation by requiring sufficient factual allegations "to raise a right to relief above the speculative level" so as to "nudge[] the[] claims across the line from conceivable to plausible." Twombly, 500 U.S. at 555, 570; see Iqbal, 556 U.S. at 680. The Court "must accept all well-pleaded allegations in the complaint as true and draw all reasonable inferences in the plaintiff's favor." Langford v. Joyner, 62 F.4th 122, 124 (4th Cir. 2023). However, the Court is not bound to accept legal conclusions. Iqbal, 556 U.S. at 678. Thus, "when there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief." Id. at 679.

III. DISCUSSION

A. Defendants' 12(b)(1) Arguments

Because "standing is a threshold jurisdictional question" courts should address it first before moving on to the merits. See Garey v. James S. Farrin, P.C., 35 F.4th 917, 921 (4th Cir. 2022) (internal brackets and quotation omitted).

Here, Defendants argue that Plaintiffs fail to allege a sufficient injury in fact to demonstrate standing and that neither of the two statutes under which Plaintiffs bring suit—information privacy and wiretapping laws from California and Pennsylvania—can alone grant standing.

The California Information Privacy Act (hereinafter "CIPA") punishes by fine or imprisonment the following conduct:

> Any person [1] who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [2] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [3] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [4] who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . . .

Cal. Penal Code § 631(a). Courts analyzing this statute have broken it down into its four constituent clauses, as indicated by the bracketed numbers above. See, e.g., Garcia v. Build.com, Inc., No. 22-cv-01985-DMS-KSC, 2023 WL 4535531, at *4-5 (S.D. Cal. July 13, 2023). As is relevant here, the second clause applies to anyone "who willfully and without the

consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state." The fourth clause imposes liability on a defendant who, even if a party to the communication at issue, "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section," including aiding in a third party's violation of the second clause. Licea v. Cinmar, LLC, No. CV 22-6454-MWF (JEM), 2023 WL 2415592, at *7 (C.D. Cal. Mar. 7, 2023).

The Pennsylvania Wiretapping and Electronic Surveillance Control Act (hereinafter "WESCA"), similarly punishes anyone who, among other things, "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication." 18 Pa. Cons. Stat. § 5703(1). The statute defines "intercept" as the "acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." Id. § 5702. "[T]here is no sweeping direct-party exception to civil liability under the WESCA" and thus, where a plaintiff communicates with a defendant and a third party intercepts that communication on the defendant's behalf, the defendant cannot avoid liability by showing that the plaintiff intentionally communicated with the defendant. See Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121, 126-29 (3d Cir. 2022).

Both CIPA and WESCA provide private rights of action. Cal. Penal Code § 637.2(a) ("Any person who has been injured by a violation of this chapter may bring an action against

the person who committed the violation . . . ."); 18 Pa. Cons. Stat. § 5725(a) ("Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of [WESCA] shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication . . . ."). Moreover, neither CIPA nor WESCA is a mere procedural statute that dictates how a person or entity should handle an individual's private information. Rather, each statute punishes a violation of a pre-existing, *de facto*, and substantive right to privacy in communications and does not merely regulate how someone should attempt to safeguard that privacy. Cf. TransUnion, 594 U.S. at 427-28 ("An uninjured plaintiff who sues [without suffering any physical, monetary, or cognizable intangible harm] is, by definition, not seeking to remedy any harm to herself but instead is merely seeking to ensure a defendant's 'compliance with regulatory law' (and, of course, to obtain some money via the statutory damages). Those are not grounds for Article III standing." (internal citations omitted)).

By nature of the fact that Plaintiffs' causes of action are based on state statutes from outside of this circuit, there are few Fourth Circuit decisions analyzing them at all, let alone in the standing context. A decision from a district court in the Fourth Circuit has noted a split in authority over whether alleging a violation of CIPA alone satisfies the injury-in-fact requirement for standing:

> Even in the context of CIPA, which . . . is a state-law analogue to the Federal Wiretap Act, there is far from a consensus regarding whether statutory violations automatically give rise to concrete harm. Compare, e.g., Licea v. Am. Eagle Outfitters, Inc., No. 22-cv-1702-MWF, 2023 WL 2469630, at *3 (C.D. Cal. Mar. 7, 2023) (holding that a bare violation of CIPA is a cognizable violation of privacy rights sufficient to establish standing), Licea v. Cinmar, LLC, No. 22-cv-6454-MWF, 2023 WL 2415592, at *3 (C.D. Cal. Mar. 7, 2023) (same), Garcia v. Build.com, Inc., No. 22-CV-01985-DMS-KSC, 2023 WL

> 4535531, at *4 (S.D. Cal. July 13, 2023) (same), with Byars v. Sterling Jewelers, Inc., No. 22-cv-1456-SB, 2023 WL 2996686, at *4 (C.D. Cal. Apr. 5, 2023) (holding that CIPA violations do not constitute an injury in fact without an additional showing of harm); Lightoller, 2023 WL 3963823, at *5 (S.D. Cal. June 12, 2023) (same), and Massie v. Gen. Motors LLC, No. CV 21-787-RGA, 2022 WL 534468, at *2, 5 (D. Del. Feb. 17, 2022) (same). Neither is there a consensus that violations of the Federal Wiretap Act alone give rise to an injury in fact. Compare In re Vizio, Inc. Consumer Privacy Litig., 238 F. Supp.3d 1204, 1215-16 (C.D. Cal 2017) (finding concrete harm from Federal Wiretap Act violations due to "the close similarity between the conduct proscribed under the [Federal] Wiretap Act and the tort of intrusion upon seclusion"), with Lopez v. Apple, Inc., 519 F. Supp.3d 672, 681 (N.D. Cal 2021) (finding that plaintiffs asserting Federal Wiretap Act violations lacked standing because they did not allege non-speculative, concrete injury beyond a statutory privacy harm).

Straubmuller v. Jetblue Airways Corp., No. DKC 23-384, 2023 WL 5671615, at *3 (D. Md. Sept. 1, 2023) (internal footnote omitted). However, the United States Court of Appeals for the Ninth Circuit in analyzing CIPA's relationship to the common-law right to privacy has held:

> As to the statutory claims, the legislative history and statutory text demonstrate that . . . the California legislature intended to protect these historical privacy rights when they passed . . . CIPA. See . . . Cal. Pen. Code § 630 (noting that CIPA was passed "to protect the right of privacy of the people of this state"). Thus, these statutory provisions codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing.

In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 598 (9th Cir. 2020); accord Yockey v. Salesforce, Inc., No. 22-cv-09067-JST, 2023 WL 5519323, at *3 (N.D. Cal. Aug. 25, 2023) ("Statutes such as CIPA and WESCA thus codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing." (internal quotation omitted)); see also Doe v. Microsoft Corp., No. C23-0718-JCC, 2023 WL 8780879, at *3 (W.D. Wash. Dec. 19, 2023) (collection of non-anonymized data without consent gave rise to an injury in fact for a CIPA claim); Cinmar, 2023 WL 2415592, at *3 ("However, violations of

plaintiffs' statutory rights under CIPA, even without more, constitute injury in fact because instead of a bare technical violation of a statute, a CIPA violation involves a violation of privacy rights." (internal brackets, ellipses, and quotation omitted)).

Violations of WESCA also generally provide a basis for standing because they necessarily involve violations of a privacy interest. See James v. Walt Disney Co., No. 23-cv-02500-EMC (EMC), 2023 WL 7392285, at *2-5 (N.D. Cal. Nov. 8, 2023) (standing established in case based on CIPA and WESCA where plaintiffs alleged that their right to control information concerning his or her person was violated); Mulder v. Wells Fargo Bank, N.A., No. 2:18-cv-00029, 2018 WL 3750627, at *4 (W.D. Pa. July 10, 2018) (plaintiff had standing to bring claims for violation of his rights under WESCA by adequately pleading wiretap claim), report and recommendation adopted, No. 18-29, 2018 WL 3744821 (W.D. Pa. Aug. 7, 2018).

These analyses of standing under CIPA and WESCA comport with recent guidance from the Fourth Circuit on standing for statutory violations.

> Plaintiffs who do not have a legally cognizable injury lack standing to bring suit in federal court. Congress may, of course, "elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." Lujan v. Defs. of Wildlife, 504 U.S. 555, 578, 112 S. Ct. 2130, 119 L.Ed.2d 351 (1992). But as the Defendants correctly point out, plaintiffs cannot establish a cognizable injury simply by pleading a statutory violation. See Spokeo, Inc. v. Robins, 578 U.S. 330, 341, 136 S. Ct. 1540, 194 L.Ed.2d 635 (2016) ("Article III standing requires a concrete injury even in the context of a statutory violation.").
>
> Balancing these two rules has in the past caused some confusion, but the Supreme Court recently clarified when a statutory cause of action identifies an injury sufficient for standing purposes. In TransUnion LLC v. Ramirez, the Court explained that plaintiffs proceeding under a statutory cause of action can establish a cognizable injury by "identifying a close historical or common-law analogue for their asserted injury" for which courts have "traditionally" provided a remedy. —— U.S. ——, 141 S. Ct. 2190, 2204, 210 L.Ed.2d 568 (2021) (citing Spokeo, 578 U.S. at 341, 136 S. Ct. 1540). A plaintiff who does

> so has standing even if the precise injury would not, absent the statute, be sufficient for Article III standing purposes.

Garey, 35 F.4th at 921 (internal brackets and footnote omitted). As such, the Fourth Circuit has recognized an injury in fact that is sufficient to establish standing where the alleged harms arising from a statutory violation "are closely related to the invasion of privacy, which has long provided a basis for recovery at common law." Id. (internal quotation omitted); see also TransUnion, 594 U.S. at 425 ("Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." (internal citation omitted)); Witt v. Corelogic Saferent, LLC, No. 3:15-cv-386, 2016 WL 4424955, at *13 (E.D. Va. Aug. 18, 2016) ("Similarly, it is well-settled that Congress may create a statutory right to privacy in certain information that strengthens or replaces the common law, and citizens whose statutory right to informational privacy has been invaded may bring suit under the statute to vindicate that right.").

In conjunction with the statutory violations of CIPA and WESCA, Plaintiffs have sufficiently alleged that these violations were premised upon and resulted in unconsented-to invasions of their privacy and disclosure of their private information. (Am. Compl. ¶¶ 2-3, 25, 41, 76-77, 83-84, 86-90, 92-96, 98-100.) Taking the facts alleged in the Complaint as true, and drawing all inferences in Plaintiffs' favor, the Court reads the Complaint as alleging that the three named Plaintiffs each conducted searches on the Labcorp website regarding their own sensitive medical issues, and that as a result of Defendants' deliberate choice to install certain code on the Labcorp website, this sensitive medical information was then intercepted and

linked with their personal identifying information and transmitted to Meta and Google, where it was linked to their Facebook ID/Google ID and then used or sold for commercial purposes, all without Plaintiffs' knowledge or consent. Given these allegations, and given that Plaintiffs adequately allege violations of these privacy-protecting statutes, they have alleged a sufficiently concrete injury to bring federal suit.

In support of dismissal, Defendants argue, in essence, that invasion of privacy cannot be a basis for standing in this case because Plaintiffs have not separately alleged the elements of such a common-law tort. (Defs.'s Br. [Doc. #79] at 9-12.) The Fourth Circuit, with the Supreme Court's decision in TransUnion in mind, has rejected just such an argument.

> [F]oreshadowing TransUnion, we recently rebuffed a nearly identical standing challenge in a case arising under [a statutory cause of action that] provides a private right of action against offenders. . . .
>
> We acknowledged [in Krakauer v. Dish Network, L.L.C., 925 F.3d 643 (4th Cir. 2019)] that although [a statutory cause of action] provides claims that differ from common law privacy torts, [Supreme Court precedent] does not require us to import the elements of common law torts, piece by piece, into any scheme Congress may devise. Rather, we concluded that our inquiry focuses on types of harms protected at common law, not the precise point at which those harms become actionable. . . .
>
> Applying the same analysis as Krakauer, we reach the same result. The Plaintiffs have alleged a legally cognizable privacy injury. See, e.g., Garey Second Am. Compl. ¶ 127 ("Each Plaintiff sustained actual damages by having his or her privacy invaded by Defendants' knowingly obtaining his or her name and address from a motor vehicle record for an impermissible purpose in violation of law."). The Defendants point out some differences between the common law privacy torts and the [statutory cause of action], but our inquiry does not require an exact duplicate in American history and tradition. At bottom, the [statute] is aimed squarely at the right of the plaintiff, in the phrase coined by Judge Cooley, to be let alone. Therefore, the Plaintiffs have Article III standing to pursue claims for damages.

Garey, 35 F.4th at 922 (internal brackets, citation, and quotation omitted).

Because CIPA and WESCA provide for liability for facilitating third-party invasion of privacy, and because Plaintiffs have sufficiently alleged that they did not consent to their private information being diverted by Defendants to third parties, Plaintiffs have adequately alleged a concrete invasion-of-privacy harm arising from Defendants' alleged violation of these California and Pennsylvania statutes. For these reasons, Defendants' motion to dismiss for lack of standing should be denied.

B. Failure to State a Claim

i. Rule of lenity

Defendants contend that the Amended Complaint should be dismissed because, under the rule of lenity, it is not clear that CIPA and WESCA should apply to their alleged conduct.

Where, as here, a court's "analysis involves a statute whose provisions have both civil and criminal application, [the] task merits special attention" because the court's "interpretation applies uniformly in both contexts." WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (citing Leocal v. Ashcroft, 543 U.S. 1, 11 n. 8 (2004)). In this situation, a court should follow "the canon of strict construction of criminal statutes, or rule of lenity." Id. (quoting United States v. Lanier, 520 U.S. 259, 266 (1997)). "In other words, in the interest of providing fair warning of what the law intends to do if a certain line is passed, [a court] will construe this criminal statute strictly and avoid interpretations not clearly warranted by the text." Id. (internal quotations omitted). However, "the rule of lenity is a last resort, not a primary tool of construction and to invoke the rule, we must conclude that there is a *grievous* ambiguity or uncertainty in the statute." Hosh v. Lucero, 680 F.3d 375, 383 (4th Cir. 2012) (internal brackets and quotations omitted).

As noted above, CIPA applies to anyone "who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done" the act of "willfully and without the consent of all parties to the communication, or in any unauthorized manner, read[ing], or attempt[ing] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable." WESCA similarly applies to anyone who intentionally "procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication." While this language may be broad, it is not as a result ambiguous. The statutes prohibit aiding anyone in reading or learning the contents or meaning of any wire or electronic message while in transit without consent. Plaintiffs allege that Defendants aided Meta and Google in reading and learning the contents and meaning of their electronic messages to Defendants, via interception of the messages while in transit over the internet, without consent.

Defendants have pointed to no specific ambiguities, let alone grievous ones, in the statutes at issue here and have not raised any specific doubts about the applicability of CIPA or WESCA to the conduct in this case. (Defs.'s Br. at 13-14.) Rather, Defendants merely allege that "Plaintiffs have not shown that either statute 'plainly' imposes penalties for [Defendants'] alleged conduct." (Defs.'s Br. at 14.) Without a more specific argument from Defendants with legal support, the Court declines to proactively search for an ambiguity in the statutes.

At this stage, the statutes appear to apply, at least facially, to the conduct alleged, when the allegations in the Amended Complaint are accepted as true. In any event, as Plaintiffs point out (Pls.'s Br. [Doc. #85] at 23), federal courts have routinely applied CIPA and WESCA

to similar scenarios or, at a minimum, have engaged with the statutes under the assumption that they applied to private parties in civil suits. See, e.g., In re Facebook, 956 F.3d at 598-99, 601, 606-08; Doe v. Microsoft Corp., 2023 WL 8780879, at *7-9; Vonbergen v. Liberty Mutual Ins. Co., No. 22-4880, 2023 WL 8569004, at *9-10 (E.D. Pa. Dec. 11, 2023); James, 2023 WL 7392285, at *14; Doe v. DLP Conemaugh Mem'l Med. Ctr., LLC, No. 3:23-CV-110, 2023 WL 5993016, at *1, *3-4 (W.D. Pa. Sept. 15, 2023); Oliver v. Noom, No. 2:22-cv-1857, 2023 WL 8600576, at *6 (W.D. Pa. Aug. 22, 2023); Popa, 52 F.4th at 131; Ades v. Omni Hotels Mgmt. Corp., 46 F. Supp. 3d 999, 1018 (C.D. Cal. 2014). Thus, for purposes of a Motion to Dismiss, Plaintiffs' similar allegations fall, at least facially, within the reasonable scope of the statutes and there is therefore no reason to find that the rule of lenity categorically bars such private causes of action.

For these reasons, and "[b]ecause there are no doubts to resolve at this stage, the Court declines to review [Defendants'] additional argument regarding the rule of lenity," without prejudice to Defendants' raising this issue again at a later stage. See Branca v. Ocwen Loan Servicing, LLC, No. CV 13-7502 BRO (Ex), 2013 WL 12120261, at *12 (C.D. Cal. Dec. 27, 2013) (CIPA case); see also James, 2023 WL 7392285, at *14 ("Assuming the rule of lenity applies to this civil action [raising CIPA and WESCA claims] because the predicate statute imposes criminal liability, this argument is not particularly compelling [because] WESCA uses broad language and engaging in a 'hyper-technical reading of the statute' is inconsistent with what is presumably the purpose of the statute, *i.e.*, to 'prohibit unauthorized artificial interception of communication in an era of changing technologies.'" (quoting United States v. Hutchins, No. 17-CR-124, 2018 WL 5313772, at *12-37 (E.D. Wisc. Oct. 26, 2018))).

ii. Contents of communications

Defendants next argue that dismissal is appropriate because Plaintiffs have not adequately alleged that the contents of their communications were intercepted. (Defs.'s Br. at 14-16.) In support of this argument, Defendants cite legal authority for the proposition that "webpage titles, webpage keywords, the date and times of website visits, IP addresses, page visits, purchase intent signals, and add-to-cart actions" do not amount to the contents of any communication. (Defs.'s Br. at 14 (quoting Katz-Lacabe v. Oracle Am., Inc., No. 22-cv-04792-RS, 2023 WL 2838118, at *9 n.9 (N.D. Cal. Apr. 6, 2023)).) Importantly however, Defendants do not allege that the content of search queries do not constitute communications. Rather, Defendants argue that Plaintiffs have failed to adequately allege that the contents of these searches were in fact intercepted. (Defs.'s Br. at 15-16; Defs.'s Reply Br. [Doc. #91] at 5-7.) However, whether Plaintiffs are ultimately able to prove that the contents of their search-based communications were sent to third parties without their consent, they have adequately alleged so.

Unlike the situation Defendants point to in Cousin v. Sharp Healthcare, No. 22-CV-2040-MMA (DDL), 2023 WL 4484441, at *3 (S.D. Cal. July 12, 2023), Plaintiffs here allege that they accessed the Labcorp website at the time that the tracking tools were deployed and entered search terms regarding their sensitive medical issues—some of which are given as examples—that the tracking tools then surreptitiously rerouted to Meta and Google with Plaintiffs' personal identifiers. Because the Amended Complaint, fairly read in Plaintiffs' favor, alleges that these transmissions were automatic and not selective during the relevant times described, the allegation that Plaintiffs entered search terms necessarily means that the

content of these search queries were sent to Meta and Google. Thus, the Amended Complaint reasonably alleges that Plaintiffs entered search terms on the website and that all searches related to their "sensitive medical issues" were rerouted to Meta and Google with their personal identifiers as a result. (Am. Compl. ¶¶ 83-84, 86-87, 89-90, 92-93, 95-96, 98-99.)

Any further issues regarding the nature of the sensitive medical issues and the specific search terms, the full nature of how these searches were conducted, and what role Defendants played in receiving or responding to them will be developed more fully during discovery, after which this issue can be better addressed. See Doe v. Meta Platforms, Inc., No. 22-CV-03580-WHO, 2023 WL 5837443, at *3 (N.D. Cal. Sept. 7, 2023) ("[W]hile a URL that includes 'basic identification and address information' is not 'content,' a URL disclosing a 'search term or similar communication made by the user' 'could constitute a communication' under [a wiretapping] statute." (quoting In re Zynga Priv. Litig., 750 F.3d 1098, 1108-09 (9th Cir. 2014))).

iii. Defendants' intent

Defendants next argue that the Amended Complaint does not adequately allege that they intended that Meta and Google would be able to intercept the contents of any communications with the Labcorp website. (Defs.'s Br. at 16-18.) Defendants appear to argue that an allegation that they "implemented" Meta's and Google's respective computer code in a way that then "permitted" these third parties "to intercept and use" Plaintiffs' search terms is insufficient to show that Defendants "intended to facilitate the transmission of the contents of Plaintiffs' communications." (Defs.'s Br. at 17.) While it may be true that a company does not intend a third party's wrongs when the third party merely exploits the company's system

to allow the third party's subsequent unrelated wrongs, that is not what is alleged in this case. As alleged in the Complaint, Defendants did not simply place computer code on its website which then gave rise to the possibility that Meta and Google could ultimately access information from that website. As alleged in the Amended Complaint, Defendants deliberately placed proprietary Meta and Google code on its website which by design automatically redirected all relevant information at issue in this case to those third parties. (Am. Compl. ¶¶ 2-3, 13, 22-25, 27-34, 38-39, 42-45, 47-53, 56, 58-75.) Moreover, the Complaint alleges that in both instances, Defendants intentionally placed the code on its website and modified it to target even more information than the default parameters programmed by Meta and Google, thus showing that the tracking tools' appearance on the website was a result of Defendants' active choice to place them there and not as a potentially inadvertent mistake while being unaware of what the code did. (Am. Compl. ¶¶ 27, 46.) Under these circumstances, and taking all allegations as true and making all reasonable inferences in Plaintiffs' favor, the Amended Complaint has plausibly alleged that Defendants intended for the tracking tools to function as they were designed and to relay any search terms, with identifiers, to Meta and Google.

iv. Plaintiffs' purported consent

Defendants' next argument for dismissal is based on information outside of the Amended Complaint which purportedly shows that Plaintiffs consented to the dissemination of their search queries to Meta and Google. (Defs.'s Br. at 18-22.) In particular, Defendants allege that "Labcorp informs Website visitors, such as Plaintiffs, that it uses Google Analytics and other analytics technologies. What is more, both Google and Meta expressly disclose how

these technologies operate and require Plaintiffs' and other account holders' consent to these practices." (Defs.' Br. at 18.) In support of this argument, Defendants invite the Court to review Labcorp's, Meta's, and Google's privacy policies (Defs.' Br. at 19-22), and have filed a separate motion asking the Court to consider these policies as integral to the Amended Complaint or to otherwise take judicial notice of them (Defs.'s Mot. for Judicial Notice [Doc. #75]).

Additionally, Defendants argue that at least Meta's privacy and cookies policies are integral to the Amended Complaint because Plaintiffs cited to them in footnotes. (Defs.'s Mot. for Judicial Notice Br. [Doc. #76] at 4 (citing Am. Compl. ¶¶ 29, 33).)

Even if the Court were to assume that these policies were integrally related to the Amended Complaint and even if they were all dated within the relevant time period of this case—which they are not—consideration of them on a motion to dismiss for the purpose Defendants propose would still be inappropriate.[2] Considering these privacy policies—which as presented merely show a snapshot in time of what the policies were on certain dates—would resolve neither what, if any, privacy policies were in place at the time Plaintiffs visited Defendants' websites nor, crucially, how or if Plaintiffs even saw or interacted with them, let alone affirmatively consented to their conditions. To the extent Plaintiffs necessarily had to

---

[2] Defendants have included and rely on seven documents which are variously dated between January 5, 2022, and July 1, 2023:

> Meta's privacy policy, dated January 1, 2023 [Doc. #77-1];
> Meta's cookies policy, dated October 5, 2022 [Doc. #77-2];
> Google's privacy policy, dated July 1, 2023 [Doc. #77-3];
> Google's tech policy, undated [Doc. #77-4];
> Labcorp's website privacy policy, dated April 7, 2023 [Doc. #77-5];
> Meta's terms of service, dated July 26, 2022 [Doc. #77-6]; and
> Google's terms of service, dated January 5, 2022 [Doc. #77-7].

have accepted these policies as a prerequisite to using any given website, any facts supporting this conclusion are entirely outside of the Amended Complaint and are not properly considered on the pending Motion to Dismiss. Moreover, Labcorp's privacy policy is not referenced in the Amended Complaint at all and thus there would be no basis for the Court to consider it here.

The Court has no doubt that the content of these policies and the nature in which they were, or were not, presented to and accepted by Plaintiffs will be crucial to this case going forward. However, discovery and future motions practice will be necessary to fully develop the record in order to consider and resolve any disputes about Plaintiffs' potential consent in this case. Therefore, the Court should deny Defendants' Motion for Judicial Notice [Doc. #75] and not consider these privacy policies, without prejudice to Defendants' later raising the issue of consent, on a motion for summary judgment.

In the absence of these policies, the Amended Complaint as written reasonably and affirmatively alleges that Plaintiffs did not consent to the conduct complained of here. (Am. Compl. ¶¶ 3, 25, 41, 76-77, 88, 94, 100.) Because these facts must be accepted as true, Defendants' Motion to Dismiss on the basis of consent should be denied.

v. Computer code as a device

Finally, Defendants move to dismiss the WESCA claim on the basis that the tracking tools in dispute in this case do not constitute "devices" because they are "intangible software code" and not a "physical object" as required by the statute. (Defs.'s Br. at 22-24.)[3] In support of this position Defendants cite state- and federal-court decisions from Florida for the

[3] These arguments are raised only as to the WESCA claim, not the CIPA claim.

proposition that computer code is not a device. (Defs.'s Br. at 23-24.) However, federal courts from Pennsylvania, analyzing the Pennsylvania statute, have assumed, at least at the pleading stage, that computer code interacting with a server may constitute a device, and have thus permitted discovery to further develop the issue.

> The use of the word "any" before the phrase "device or apparatus" in Section 5702 implies that the class of technology contemplated by WESCA is broad. . . .
>
> . . . .
>
> While the statutory definitions of "device" and "electronic communication" are broad, they are not limitless. They may or may not include the type of electronic data collection complained of by Popa. To prevail on a claim under WESCA, it is Popa's burden to prove that the allegedly actionable conduct falls under the purview of the statute. The nature of the conduct involved makes it less than clear at this stage. Indeed, whether the interplay between Defendants' servers and Navistone's code qualifies as a "device" or "apparatus" is a fact intensive inquiry that implicates novel questions. The discovery process will give the parties an opportunity to develop a record that contextualizes the conduct at issue in light of this statutory language.

Popa v. Harriet Carter Gifts, Inc., 426 F. Supp. 3d 108, 117, 123 (W.D. Pa. 2019) (denying motion to dismiss WESCA claim), case subsequently vacated on appeal on separate grounds, Popa, 52 F.4th at 131 n.8 (assuming that code directing communications to a server is a "device" under WESCA); see also Vonbergen, 2023 WL 8569004, at *9-10 (finding, at motion to dismiss stage, that plaintiff had sufficiently alleged that tracking software was a "device" under WESCA); Noom, 2023 WL 8600576, at *6 (finding, at motion to dismiss stage, that plaintiffs had sufficiently alleged that computer code which directed information to a server was a "device" under WESCA).

The Amended Complaint alleges that the tracking tools at issue in this case function as computer codes that send information, including the contents of search queries and personal

identifiers, to servers. (Am. Compl. ¶¶ 28, 45.) With the case law from the Third Circuit interpreting the Pennsylvania WESCA law in mind, the Court finds that Plaintiffs have sufficiently alleged that a device was used to intercept their communications here. As in Popa, whether Plaintiffs will be able to prove that these interactions between code and server occurred in a way to constitute a device will be discovery-dependent, but Plaintiffs' allegations are sufficient to survive a motion to dismiss.

IV. INTIAL PRETRIAL CONFERENCE

Plaintiffs have also filed a Motion [Doc. #97] requesting that the case be set for Initial Pretrial Conference. In light of this Recommendation, that request will be granted and the case will be set for Initial Pretrial Conference on Thursday, September 26, 2024 in Winston-Salem. The Parties' Rule 26(f) Report(s) should include a schedule for briefing the request for class certification and a proposal for how that will fit into the discovery schedule.

V. CONCLUSION

IT IS THEREFORE RECOMMENDED that Defendants' Motion to Dismiss [Doc. #78] be denied, and that Defendants' Motion for Judicial Notice [Doc. #75] be denied.

IT IS ORDERED that Plaintiff's Motion for Initial Pretrial Conference [Doc. #97] is GRANTED, and this case is set for Initial Pretrial Conference on Thursday, September 26, 2024, at 9:30 a.m. at the Federal Courthouse in Winston-Salem, North Carolina.

This, the 8th day of August, 2024.

Joi Elizabeth Peake
United States Magistrate Judge